ABSTRACT:

The invention proposes an encryption method wherein a cryptographic sub-operation is performed on digital data which are stored as at least one data bit word in a storage cell (10) or a register and wherein successful crypto analysis by observation of current consumption of a data processing apparatus is effectively prevented by writing a data bit word based on random numbers into a storage cell (10) before a data bit word is written therein.